CHAPTER – II

HIGHLIGHTS OF INFORMATION TECHNOLOGY ACT

Since the beginning of civilization, man has always been motivated by the need to make progress and better the existing technologies. This has led to tremendous development and progress which has been a launching pad for further developments. Of all the significant advances made by mankind from the beginning till date, probably the most important of them is the development of Internet.\(^1\) With the advancement of technology, new methods of crime are coming to the fore. Criminals and anti-social elements with their ingenuity manage to exploit the technological developments for illegal pecuniary gain or plain pleasure causing monetary loss as well as mental disturbance to the innocent citizens. In order to protect the fundamental rights of the law abiding citizens, it becomes inevitable for the state to intervene and regulate human activity as well as legislate on various subjects and ensure enforcement of the legislations in letter and spirit through the police, thus making the police an essential part of governance by the state.

As society relies increasingly on computers, the amount of crime perpetrated with the machines has risen in kind. To law enforcement’s delight, electronic records have proved to be a fertile ground for detectives.\(^2\)

The Internet

Internet is one of the most wonderful inventions of the last century. Now, it has become integral part of our life and it is continuously making human life

---

\(^{1}\) www.mondaq.com browsed on 11\(^{th}\) February 2012.

easier and simpler in various ways. From information accessing to money transfer, all kinds of tasks are performed using the internet. Today, more and more people are relying on online banking and online shopping.

There are many networks that exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. This requires connecting together different, and frequently incompatible networks, to make the connection and provide the necessary translation, both in terms of hardware and software. A collection of interconnected networks is called an internetwork or just internet. An internetwork is formed when distinct networks are connected together.

“Internet” refers to the global formation system that – (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suits or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

New communication systems and digital technology have made dramatic changes in the way we live and the means to transact our daily business. Businessmen are increasingly using computers to create, transmit and store information in electronic form instead of traditional paper documents. It is cheaper, easier to store and retrieve speedier to communicate. Although people are aware of the advantages which the electronic form of business provides, people are reluctant to conduct business or conclude transaction in the electronic form
due to lack of appropriate legal framework. Electronic commerce eliminates the need for paper based transactions. The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance are the requirements of writing and signature for legal recognition. At present, many legal provisions assume the existence of paper based records and documents which should bear signatures. The Law of Evidence is traditionally based upon paper-based records and oral testimony. Hence, to facilitate e-commerce, the need for legal changes has become an urgent necessity.3

The latest threat to privacy, property and peace of individuals all over the world is from abuse of technology relating to computers, their network or hardware devices, where the computer or device may be agent of crime, the facilitator of the crime or the target of crime.

However, the rapid evolution of Internet has also raised numerous legal issues and questions. As the scenario continues to be still not clear, countries throughout the world are resorting to different approaches towards controlling, regulating and facilitating electronic communication and commerce.4

The Way Internet Works

There are many types of internet traffic. The most familiar is related to the World Wide Web, which was first developed at the European Organization for Nuclear Research (CERN) at the end of 1980s. The web was first conceived as a system of documents containing links to other documents – a concept known as ‘hypertext’ that had been proposed as early as the 1930s.

---

3 www.cactusblog.files.wordpress.com browsed on 30th September 2013.
4 www.mondaq.com browsed on 11th February 2012.
By clicking on a link in a web browser, a series of operations is initiated which results in the display of a new webpage on a computer. The first step is to translate the human-readable name of a service, such as www.target.com, to the numerical Internet Protocol (IP) address that computers can use to locate other computers on the internet. This is done using a Domain Name System (DNS) server, usually operated by the user’s Internet Service Provider (ISP), whose location is usually provided to the user’s computer when they first connect. Several alternative DNS servers are available – well known examples are operated by Open DNS, as well as Google.

**Benefits of Internet**

The Internet can be used for a variety of purposes from anywhere in the world. Some of the users are:

- To exchange e-mail instantly with friends or institutions in India or abroad.
- To participate in teleconferences with people on topics of interest or research problems.
- To find out educational information from universities worldwide, libraries and book stores.
- To surf on different topics for pleasure.
- To read about interesting sports and games.
- To find out information on agriculture, irrigation, crops, seeds, pesticides, labour, health, diseases, medicines, livestock and many other rural problems.
- To use it for e-commerce, e-governance, e-banking, e-medicines etc.
• To interact with government departments on registration, taxation, water & drainage, gas, income tax etc.,

• To improve literacy, adult education, gender equality and promote cultural heritage.

• To search on-line library catalogues for bibliographic data and other databases for textual data.

• To have access to electronic journals, newsletters and in-house information of many organizations and institutions.

• To communicate with others through the sites of social network.

Cyber Space

The New Shorter Oxford Dictionary explains the expressions ‘Cyber Space’ as ‘notional environment within which electronic communication occurs especially when represented as the inside of a computer system, space perceived as such by an observer, but generated by a computer system and having no real existence, the space of virtual reality’.

Definitions of Cyber Crime

The Information Technology Act, 2000 (I.T. Act) defines Cyber Crime as “the act of a person which is intentionally conceals or destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or network is cyber crime”.

An act or omission, which is punishable under the law in force, is known as crime. The same explanation is also applicable to cyber crime. But, there is no
legal definition for cyber crime. The purpose of adding the word cyber with crime is only to indicate that the computer has been used to commit an illegal act and to caution the users for safeguarding the digital evidence, which is of fragile in nature. In short, cyber crime can be known as digital crime. In literal sense, cyber was a word coined by William Gibson in his 1984 fictional novel ‘Neuromancer’. Cyber is the prefix relating to the worldwide field of electronic communication. Crimes involving stealing, fabricating, leaking or circulating forbidden digital information is collectively branched under the umbrella term cyber crime.\(^\text{5}\)

Cyber crimes can be broken down into two types through the Information Technology Act does not make such a distinction.

The first type of cyber crimes are actually pranks in which the intention of the perpetrator is merely to create a nuisance. Thus, he may hack into a website and deface it, or break into one’s email account and read private mail, or post obscene material. This type of offender is generally a computer buff who is essentially trying to show off his prowess such people get a kick by doing things which are arcane to most people. They may not really intend to derive any criminal, financial or sexual benefit out of their activities.

The second type of cyber crime is real crime in the sense that the offender intends to derive pecuniary or sexual benefit by it. Thus, he may indulge in credit card or bank fraud, selling of secret commercial or security information obtained by hacking or helps in transmission of criminal information. Whether he is a prankster or a real criminal, the offender is necessarily a person who has a great deal of knowledge of computer, networks, security system and the Internet. It can

---

be safely presumed that he knows a great deal more than perhaps the best investigators and can easily take them for a ride. Cyber crime may be said to be those species of the conventional crime and there, either the computer is an object or subject of the conduct constituting crime.

Cyber crimes share three elements:

1. Tools and techniques to perpetrate a crime.
2. Approach or methodology for executing the criminal plan – known as vector.
3. Crime itself that is the end of those plans and activities (a cyber crime is the ultimate objective of the criminal’s activities).

Cyber crimes are committed mostly by persons who are said to be learned and hence, it is called as white collar crime. Cyber crimes are very serious threat in the modern era and for the times to come and pose one of the most difficult challenges before the law enforcement machinery, especially to investigate, collect evidence, and to penalize. In the information age, the rapid development of computers, telecommunications and other technologies has led to the evolution of new forms of transnational crimes known as “cyber crimes”. Cyber crimes have virtually no boundaries and may affect any country in the world. A generalized definition of cyber crime may be “Unlawful acts where in the computer is either a tool or target or both”. Most cyber crimes do not involve violence, but rather greed, pride or play on some character weakness of the victims. Although it is difficult to identify the culprit, as the Net can be a vicious web of deceit and can be accessed from any part of the globe. The damage caused are almost an unrealizable, expect for certain financial damage which runs in billions every year and shall create irreplaceable loss to the individuals and corporate. A cyber crime
is generally a domestic issue, which may have international consequences in most of the instances.⁶

**Types of Cyber Crimes**

There are several Cyber Crime which some of them detailed as follows:

**Hacking**

Hacking is the unauthorised access to computer system or networks. Hackers are people with sufficient technical ability to gain access to another person’s computer or to a network through the use of stolen passwords, or interference technology which provides access to networks and individual computers.⁷

**Cyber Terrorism**

In the context of Information Technology security, terrorists can come in many forms such as politically motivated, anti-government, anti-world trade and pro-environmental extremists. The term cyber terrorism was coined in 1996 by combining the terms cyber space and terrorism. Cyber attacks may be carried out through a host of technologies, but have an attack pattern that may be modelled.⁸

**Identity Theft**

Identity theft involves acquiring key pieces of someone’s identifying information in order to impersonate them and commit various crimes in that person’s name. Besides basic information like name, address, telephone number, identity thieves look for social insurance numbers, driver’s license numbers, bank

---

⁶ *Criminal Investigation Department Review, Tamil Nadu – January 2008*: Types of Cyber Crime – An Overview, article submitted by Mr. Syed Umarrathab, UGC Doctoral Research Scholar, Department of Criminology, University of Madras.


account numbers, birth certificates or passports etc. These informations enable them to commit numerous forms of fraud.\(^9\)

**E-bombing**

A programme planted surreptitiously with intent to damage or destroy a system in some way – for example to erase a hard disk or cause it to be unreadable to the operating system through Trojan horse, virus, worms.\(^10\)

**E-mail spoofing**

Spoofing is the process of pretending to be another person or process with the goal of obtaining unauthorized access. E-spoofing usually done by using a bogus IP address, but it could be done by using someone else’s authentication credentials.\(^11\)

**Cyber Stalking**

Stalking generally involves harassing or threatening behavior repeatedly such as following a person, appearing at a person’s home or business, making harassing through phone calls or vandalizing a person’s property. Cyber stalking is one of the most common crime which are commenced on internet and using the internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse.\(^12\)

**Software Piracy**

According to Microsoft Company, software piracy is defined as “the copying of a computer software programme without the permission of the copyright owner”. Certain reports indicated that more than $7.5 billion worth of

---


\(^10\) *Microsoft Internet & Networking*, Prentice-Hall of India, New Delhi, 2003, p.29.


\(^12\) www.ijecs.in browsed on 29\(^{th}\) May 2014.
American software illegally copied and distributed around the world each year. In China, 96% of all business software is pirated, but in Vietnam, it is peaked to 98%.  

Digital Forgery

Digital technology facilitates to forge a document through printers and scanners by developing counterfeit currencies, postal cards, revenue stamp, mark sheet, birth certificate etc.  

Cyber Squatting

It has similarities with old strategy or registering trademarks only to prevent others from using it. Here, the site names in the internet are blocked and then traded by unscrupulous persons for monetary benefits. Well-known celebrities, governmental establishments etc., are the victims of these activities.  

Child Pornography

Paedophiles and child pornography is nothing unknown to the world. But, the internet has made it so easy for the paedophiles to organize and distribute the offensive materials throughout the world. Also, the paedophiles makes them vulnerable of exploitation.  

Data Diddling

This kind of an attack involves altering new data just before a computer processes it and then changing it back after the processing is completed. The

---

13 www.cjimagazine.com browsed on 29th May 2014.
16 Ibid, p.64.
Electricity Board faced similar problem of data diddling while the department was being computerised.\textsuperscript{17}

**Web Jacking**

This term is derived from the term hijacking. In this kind of offence, the hacker gains access and control over the website of another. He may even mutilate or change the information on the site.\textsuperscript{18}

**Distributed Denial of Service (DDoS) Attack**

This is an attack in which thousands of separate computers, which are usually part of a botnet, bombard a target with bogus data to knock it off the net. These attacks have been used by extortionists who threaten to knock a site offline unless a hefty ransom is paid.\textsuperscript{19}

Apart from the above, other types of cyber crimes are Online Gambling, Intellectual Property crimes, Cyber Defamation, Internet Time Thefts, Theft of Computer System, Physically Damaging a computer system, etc.

**Cyber Law Initiation**

To penalise the cyber offenders and to prevent cyber crimes, the step to create Information Technology Act was initiated. The first comprehensive initiative of law on computer crime was a staff study by the U.S. Senate Government Operations Committee in February 1977. This staff study addressed and recommended that legislation should be considered that would prohibit unauthorized use of computers. The Chairman of this Committee was Senator Ribicoff and introduced this in 1977 which was called as Ribicoff Bill. This Bill was the first proposal for Federal Computer Crime legislation in the U.S., but was


\textsuperscript{19} www.brighton.ac.uk browsed on 17\textsuperscript{th} January 2016.
not adopted. This pioneer proposal became the model legislation in State computer crime legislation in the United States and created awareness all around the world.20

Cyber law is a term used to describe the legal issues related to use of communication technology, particularly in the “cyber space”. It is less a distinct field of law in the way that property or contract are, as it is an inter-section of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world. Cyber law is important because, it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyber space. As such, a single transaction may involve the laws of at least three jurisdictions viz. the laws of the nation in which the user resides, the laws of the nation where the server hosting the transaction is located, and the laws of the nation which apply to the person or business with whom the transaction takes place. So a user in one of the United States conducting a transaction which another user in Britain through a server in Canada could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.21

Importance of Cyberlaw

The draft cyber security policy document put out by the Department of Information Technology (DIT) for public discussion is an important step, but it is essentially a departmental effort, not taking a whole-of-government approach.

DIT does not have jurisdiction over departments. The document lists a number of major stakeholders, including: (1) National Information Board (NIB); (2) National Crisis Management Committee (NCMC); (3) National Computer Security Centre (NCSC); (4) Ministry of Home Affairs (MHA); (5) Ministry of Defence; (6) Department of Information Technology (DIT); (7) Department of Telecommunication (DoT); (8) National Cyber Response Centre (NCRC); (9) Indian Computer Emergency Response Team (CERT-In); (10) National Information Infrastructure Protection Centre (NIIPC); (11) National Disaster Management Authority (NDMA); (12) Standardisation, Testing and Quality Certification (STQC) Directorate; and (13) Sectoral CERTs. However, only CERT-In is mandated under the IT Amendment Act, 2008 to serve as the national agency in charge of cyber security. The Act also provided for national nodal agency for protection of Confederation of Indian Industry (CII), but it is not clear whether such an organisation exists other than on paper; National Disaster Management Authority (NDMA) and some others play only a peripheral role; and many of the sectoral CERTs are yet to come up. In the meantime, real oversight over cyber security said to be distributed amongst the Ministries of Communication and Technology, Home Affairs, Defence and the office of the NSA.22

At this juncture, it is relevant for us to understand what the IT Act, 2000 offers and its various perspectives.

Legislation and Frameworks

Legal measures play a key role in the prevention and combating the cyber crime. These are required in all areas, including criminalization, procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability. At the national level, both existing and new (or planned), cyber crime laws most often concern criminalization and indicating a predominant focus on establishing specialized offences for core cyber crime acts.\(^{23}\)

The last two decades have seen significant developments in the promulgation of international and regional instruments aimed at countering cyber crimes. These include binding and non-binding instruments.

Globally, 82 countries have signed and/or ratified a binding cyber crime instrument. In addition to formal membership and implementation, multilateral cyber crime instruments have influenced national laws indirectly, through use as a model by non-States parties, or via the influence of legislation of States parties on other countries.\(^{24}\)

Functions of cyber crime legislation

1. Setting clear standards of behaviour for the use of computer devices.
2. Deterring perpetrators and protecting citizens.
3. Enabling law enforcement investigations while protecting individual privacy.
4. Providing fair and effective criminal justice procedures.


5. Requiring minimum protection standards in areas such as data handling and retention.
6. Enabling co-operation between countries in criminal matters involving cyber crime and electronic evidence.\textsuperscript{25}

**History**

The United Nations General Assembly by resolution in No.A/RES/51/162 dated 30\textsuperscript{th} January 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This is referred to as the UNCITRAL Model Law on E-Commerce.\textsuperscript{26}

**INFORMATION TECHNOLOGY ACT, 2000**

Due to immense increase in the use of internet and dependency of individuals in every field, a number of new crimes related to Computer and other gadgets based on internet have evolved in the society. Such crimes where use of computers coupled with the use of internet is involved are broadly termed as Cyber Crimes.\textsuperscript{27}

National Association of Software and Services Companies (NASSCOM) is one of the main organisation for paving the way for enacting Information Technology Act, 2000. To improve the commercial ability of our nation, the modern methods have to be followed in e-commerce. Existing laws were not enough for these kinds of improvements. For recognizing this, an act to be implemented. Hence, the Government of India accepted the version of

\textsuperscript{25} Ibid.
\textsuperscript{26} www.uncitral.org browsed on 10\textsuperscript{th} January 2016.
\textsuperscript{27} www.mondaq.com browsed on 11\textsuperscript{th} February 2012.
NASSCOM. The Government also accepted the suggestion of NASSCOM in creating this law.

The internet was considered as main for passing the information worldwide. The famous advocate Alan Chudin who was the legal advisor for major computer concerns worldwide had said that India is having lot of intellectual talents and law has to be created by India in the field of information technology and e-commerce. He also stated that by creating this law, India will gain lot of benefits. Hence, it was realised that creation of new law for internet was necessary. Following the UN Resolution, the Government of India has passed its first Cyber law, the **Information Technology Act, 2000** which provides the legal infrastructure for E-Commerce in India. The said Act has received the assent of the President of India and has become the law of the land in India on October 17, 2000. India is 12th nation in the world to adopt cyber laws.\(^\text{28}\)

The effort was taken in the year 1998 itself. Alan Chudin was also one amongst the main person for enacting this law.\(^\text{29}\)

**Provisions**

The Information Technology Act, 2000 comprises 94 sections which is divided into 13 chapters. The chapters cover digital signature, electronic governance, attribution, acknowledgement and dispatch of electronic records, security of electronic record and digital signatures, regulation of certifying authorities, duties of subscribers to digital signature certificates, penalties, cyber regulations appellate tribunal, offences and liabilities of network service providers. The Act has four schedules that lay down the relative amendments to be

\(^{28}\) www.sethassociates.com
in the Indian Penal Code, Indian Evidence Act, Banker’s Book Evidence Act, and the Reserve Bank of India Act.\textsuperscript{30}

This is an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.\textsuperscript{31}

The object of the Information Technology Act, 2000 as defined therein is as under:

“to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.”\textsuperscript{32}


\textsuperscript{31} www.cactusblog.files.wordpress.com browsed on 30th September 2013.

\textsuperscript{32} www.mondaq.com
Key Progress Features of the Act

The Information Technology Act, 2000 provides a much-needed legal framework for electronic transactions in India. Some of its key progress features can be summarised as follows:

- First of all, these provisions have approved e-mail as a valid and legal form of communication in India that can be duly produced and approved in a Court of law.
- Companies are able to carry out electronic commerce using the legal infrastructure provided by the Act.
- The Act bestows legal validity and sanction on digital signatures.
- The Act allows companies to become certifying authorities that may issue digital signature certificates.
- The Act allows the government to issue legal notifications on the internet, a first step towards e-governance.
- The Act enables companies to file any form, application or other document with any office, authority, body or agency owned or controlled by the government in such electronic formats as may be prescribed by the government.
- The Act also addresses important issues of security that are critical for the success of electronic transactions. It includes a legal definition of the concept of secure digital signatures that must undergo a security procedure as stipulated thereunder.
The Act offers companies a statutory remedy in case anyone should break into their computer systems or network and cause damage or copy data. The remedy provided by the Act, is in the form of monetary compensation for damages for exceeding Rs.1 Crore.33

The Act has extra-territorial jurisdiction to cover any offence committed outside the country by any person.

**The Indian Penal Code, 1860**

The Indian Penal Code was amended by inserting the word ‘electronic’ thereby treating the electronic records and documents on a par with physical records and documents. The sections dealing with false entry in a record or false document etc. (e.g. 192, 204, 463, 464, 468 to 470, 471, 474, 476 etc.) have since been amended as ‘electronic record and electronic document’ and thereby bringing within the ambit of IPC. After the amendment, the investigating agencies file the cases/charge-sheet quoting the relevant sections from IPC under section 463, 464, 468 and 469 read with the ITA/ITAA under Sections 43 and 66 like offences to ensure the evidence and/or punishment can be covered and proved under either of these under both legislation.34

**Indian Evidence Act, 1872**

Under the normal circumstances, secondary evidence is not admissible in the court of law. But, the electronic documents including computer print-outs which are not original are admissible in the court of law due to the amendment to Section 65 (B) of Indian Evidence Act. For the admission of print out etc., the

---


34 www.mondaq.com browsed on 11th February 2012.
system administrator has to issue a certificate as stipulated in the Section 65 (B) of IEA. The conditions prescribed in the Section require the computer to be in regular, lawful and routine usage. It also requires the ensuring of raw data feed to be regular; and computer operation should have been normal. Derived information produced in court is subject to the ordinary course of operations. If more than one computer is produced as evidence, all computers or evidence contained in them, shown during the court proceedings should be certificated by the Administrator.

Prior to enactment of ITA, all evidences in a court were in the physical form only. After existence of ITA, the electronic records and documents were recognized. The definition part of Indian Evidence Act was amended as “all documents including electronic records” were substituted. The important amendment was seen by recognition of admissibility of electronic records as evidence as enshrined in Section 65B of the Act.

**The Bankers’ Books Evidence (BBE) Act, 1891**

Before passing of ITA, a bank was supposed to produce the original ledger or other physical register or document during evidence before a Court. After enactment of ITA, the definitions part of the BBE Act stood amended as “bankers’ books’ include ledgers, day-books, cash books, account books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device”. The above amendment in the provisions in BBE Act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided, such print-out
or electronic document is accompanied by a certificate in terms as mentioned above.

Digital signatures have been accorded legal acceptance by the I.T. Act. The Controller of Certifying Authorities, set up to implement the IT Act, has issued licences to four players who can issue digital signatures. These are Safescrypt Limited, National Informatics Centre (NIC), Institute for Development and Research in Banking Technology (IDRBT) and Tata Consultancy Services (TCS).

Later, in July 2001, a set of laws known as the Information Technology (Certifying Authority) Regulations, 2001 were issued by the Government of India. These regulations detail the functioning of the certifying authorities in issuing digital signatures. These rules specify the manner in which information has to be authenticated by means of digital signatures, the creation and verification of digital signatures, licensing of certification authorities and the terms of the proposed licenses to issue digital signatures.

The Information Technology (Amendment) Act, 2008

The Information Technology (Amendment) Act, 2008 (ITAA) was passed by the two houses of the Indian Parliament on December 23 and 24, 2008 and came into effect from 27th October 2009. It has extended the scope for the law to cover a few more cyber crimes under its ambit. The new and improved Act aims at tightening procedures and safeguards for monitoring and interception of data to prevent cyber crimes.
Salient Features of ITAA

The salient features of the amended IT Act are introduction of a system of electronic signatures on par with international law; delivery of services by service provider; corporation responsibility for data protection with the concept of reasonable security practices, recognition of Computer Emergency Response Team-India (CERT-In) as the nodal agency at the national level empowered to monitor, intercept and even block websites under specific circumstances in order to deal with computer security and situations arising from cyber attacks.35

This section also means that there is no need for a complaint and suo-moto action is possible.

Power of investigation

It is generally felt that with enactment of IT Act, 2000, the realm of investigation of computer related crimes is restricted to Deputy Superintendent of Police or officers of higher rank under section 80 of I.T. Act. This was amended in IT (Amendment) Act, 2008 that the Inspector of Police can investigate the cyber crime cases.

Section 69 empowers the Central Government/State Government/its authorized agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for

investigation of any offence. They can also secure assistance from computer personnel in decrypting data.

**CERT-IN**

Computer Emergency Response Team-India (CERT-IN) shall be the single authority for issue of instructions in the context of blocking websites. CERT-IN, after verifying the authenticity of the complaint and after satisfying that action of blocking of the website is absolutely essential, shall instruct Department of Telecommunication (DoT)-Latest Release (LR Cell) to block the website. DoT, under whose control the Internet Service Providers (ISPs) are functioning will ensure the blocking of websites and inform CERT-IN accordingly. The Director General of Police of all the State and such other enforcement agencies could approach CERT-IN.36

The blocking of website may be the need of several agencies engaged in different walks of public and administrative lives due to a variety of reasons. Explicit provision for blocking the website under the Information Technology Act, 2000 is available only in Section 67, relating to pornographic content on the website.

Such blocking can be challenged if it amounts to restriction of freedom of speech and expression. But websites promoting hate content, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography, and violent sex can reasonably be blocked since all such websites may not claim constitutional right of free speech. Blocking of such websites may be equated to “balanced flow of information” and not censorship.

---

Important Offences under ITA and ITAA and Penalties

All cyber crimes do not come under the Information Technology Act, 2000. To deal with new types of cyber crimes such as tampering of source code, hacking and publication of obscene information in electronic form, the new act can be invoked. For other type of crimes such as cheating, fraud, forgery, threat, misappropriation, defamation etc., committed by using computer, IPC and other special laws have to be invoked. For immediate reference, certain penal sections are given here for certain offences frequently witnessed.

Source code is an important asset of software companies. Computer Source Code is the listing of programmes, computer commands, design and layout. Knowledge or intention of concealment, destruction and alteration of computer source codes, which are required to be maintained, by law are the ingredients for invoking Section 65 of the I.T. Act, 2000. Punishment for this offence is three years rigorous imprisonment or fine up to Rs.2 lakhs or with both. This offence is cognizable.

Hacking has been properly defined in Section 66 as, “Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.” Further for the first time, punishment for hacking as a cyber crime prescribed in the form of imprisonment upto 3 years or with fine which may extend to Rs. 2,00,000/- or with both. This is a welcome measure as hacking has been given tremendous importance in the present day scenario. On previous occasions, the websites of the Government have been hacked into but no
legal provision within the existing legislation could be invoked to cover “hacking” as a cyber crime. It shall now be possible to try and punish hackers under section 66 of the Information Technology Act, 2000.37

Sec.66 (2) - Hacking with computer system: “whoever commits hacking shall be punished with imprisonment upto three years or with fine which may extend upto two lakh rupees, or both”.38

Sec.72 – Penalty for Breach of confidentiality and privacy : “If any person who, in pursuance of any powers conferred under this Act, Rules or Regulations made there under, has secured access to any electronic record, book register, correspondence, information, document or other material without consent of the person concerned discloses such electronic record, book, register, correspondence, information, document, or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.”

Some other sections are:

- Loss/damage to computer resource/utility – Section 66 (1).
- Obscene publication – Section 67.
- Failure of compliance/orders of certifying authority – Section 68.
- Failure to assist in decrypting intercepted by Government – Section 69.
- Unauthorised access – Section 70.

37 www.mondaq.com browsed on 11\textsuperscript{th} February 2012.
38 www.naavi.org browsed on 04-10-2013.
• Obtaining licence or digital signature certificate by misrepresentation – 71.
• Publishing false digital signature certificate – Section 73.
• Fraud Digital Signature Certificate – Section 74.

**Computer related crimes under IPC and Special Laws**

**Sec.379 IPC** – Punishment for Theft: “whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.”

**Sec.406 IPC** - Punishment for criminal breach of trust: “whoever commits criminal breach of trust shall be punished with imprisonment of either description for a term which may extend to 3 years, or with fine, or with both.”

**Sec.447 IPC** - Punishment for criminal trespass: “whoever commits criminal trespass shall be punished with imprisonment of either description for a term which may extend to three months, or with fine which may extend to five hundred rupees, or with both.”

Some other sections are:

- Counterfeiting Property Mark – 183, 482, 483, 484, 485 IPC.
- Offences by or against public servant – Sections 167, 172, 173 and 175 IPC.
- False electronic evidence – Section 193 IPC.
- Destruction of electronic evidence – Sections 204 and 477 IPC.
- Web-Jacking – Section 383 IPC.
- Bogus websites, cyber frauds – Section 420 IPC.
- Forgery of electronic records – Sections 463, 470 and 471 IPC.
Email spoofing – Sections 416, 417 and 463 IPC.

Criminal breach of trust/Fraud – Sections 405, 408 and 409 IPC.

Tampering – 489 IPC.

Counterfeiting Currency/Stamps – 489 A to 489 E IPC.

Sending defamatory messages by email – Sections 499 and 500 IPC.

Sending threatening message by email – Section 503 IPC.\textsuperscript{39}

Online sale of Drugs – NDPS Act.

Online sale of Arms – Arms Act.

The I.T. Act, 2000 does not apply to:-

1. Negotiable instrument as defined in Section 13 of the Negotiable Instruments Act, 1881.

2. Power-of-Attorney as defined in Section 1A of the Powers-of-Attorney Act, 1882.

3. Trust as defined in Section 3 of the Indian Trusts Act, 1882.

4. Will as defined in Sub-section (h) of Section 2 of the Indian Succession Act, 1925, including any other testamentary disposition by whatever name called.

5. Any contract for the sale of conveyance of immovable property or any interest in such property.

6. Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.\textsuperscript{40}

\textsuperscript{39} www.computerworld.com browsed on 10\textsuperscript{th} March 2010.

\textsuperscript{40} Saraswathi Murali: \textit{Information Technology Handbook}, Shrinikethan, Chennai, 2003, p.234
Supreme Court Ruling on Freedom of Expression

Article 19 (1) (a) of the Constitution of India, 1949, has been quoted that all citizens shall have the right to freedom of speech and expression. It has been used by the citizens of our country through social networking sites viz. Facebook, Whatsapp etc. In a landmark judgment pronounced by the Hon’ble Supreme Court of India on 24th March 2015, quashed Section 66A of the Information Technology Act, 2000 which clamped down on freedom of speech and allowed the State to arrest people posting “offensive content”. The new judgment means no one will be arrested for a Facebook post, tweet or cartoon. The court also quashed Section 118 (D) of the Kerala Police Act, a similar Act that enabled the state to arrest people. The petition against Section 66A was first filed by 23-year-old Shreya Singhal, after two girls from Palghar were arrested in 2012 when one of them made a Facebook post on a bandh called after the death of Shiv Sena leader Bal Thackeray, and the other like it. Seven other petitions, including those by People’s Union for Civil Liberties, Mouthshut.com and the Internet and Mobile Association of India followed and the SC clubbed these together.

The Supreme Court has said that the petitions against the Section “raise very important and far-reaching questions relatable primarily to the fundamental right of free speech and expression is guaranteed by Article 19 (1) (a) of the Constitution of India.” No social media posts can be taken out without a court order. The Supreme Court ruling categorized freedom of speech in three sections: for discussions, advocacy and incitement. Any expression that discusses or advocates cannot be punishable under law.  

41 www.dnaindia.com browsed on 22nd January 2016.
Cyber/Computer Crime Legislations in Various Countries

**United States of America**

The Computer Fraud and Abuse Act was enacted by Congress of USA in 1986 and the same was amended in 1989, 1994, 1996, 2001 by the USA Patriot Act, in 2002 and 2008 by the Identity Theft Enforcement and Restitution Act. The USA has also passed other enactments, which contains some or other aspects of fighting cyber crimes.\(^{42}\)

**United Kingdom**

The United Kingdom has passed various legislations to deal with cyber crimes and to regulate the transactions on cyber space. In the context of combating cyber crimes, the important Acts are: 1) The Computer Misuse Act, 1990 and 2) Regulation of Investigatory Powers Act, 2000.\(^{43}\)

**Ireland**

Ireland has passed Criminal Damages Act, 1991 to deal with damages caused to or by a computer system or network.\(^{44}\)

**People’s Republic of China**

In order to strengthen the security and the protection of computer information networks and of the internet, and to preserve the social stability, Computer Information Network and Internet Security, Protection and Management Regulations were adopted by China and it came into effect on 30\(^{th}\) February 1997.\(^{45}\)

---


Singapore

Singapore is one of those countries wherein a conscious effort was undertaken to demarcate the cyber crimes and subject them to specialized treatment. It passed the Computer Misuse Act, 1998 based on UK.\textsuperscript{46}

Australia

Australia has adopted the Cyber Crime Act, 2001 to amend the law relating to computer offences and other related purposes. This was amended in 2002.\textsuperscript{47}

\textsuperscript{46} Ibid., p.118.